

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224456

(43)Date of publication of application : 17.08.1999

(51)Int.Cl. G11B 19/04
G06F 3/06
G06F 12/14
G11B 19/12
G11B 20/10
G11B 20/12

(21)Application number : 10-025311

(71)Applicant : SONY CORP

(22)Date of filing : 06.02.1998

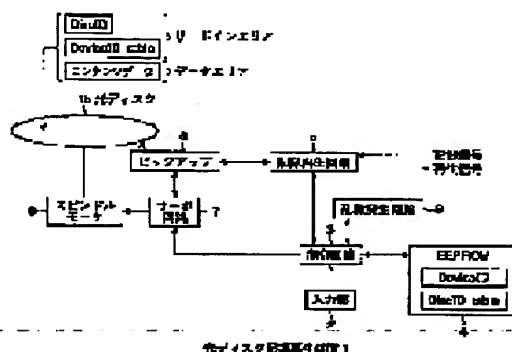
(72)Inventor : ASANO TOMOYUKI

(54) INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, PROVIDING MEDIUM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal copying of information recorded in a recording medium.

SOLUTION: A control circuit 3 reads the DiscID of an optical disk 15. A random number generating circuit 9 generates a specified random number changed for each access. The control circuit 3 writes the read DiscID of the optical disk 15 and the random number in the DiscID table of an EEPROM 4. The control circuit 3 also writes the DeviceID of an optical disk recording/ reproducing device 1 and the same random number as that described above in the DeviceID table of the optical disk 15. The control circuit 3 reads the DeviceID table and, if the read random number is not coincided with that of the corresponding DiscID table, rejects access to the user data area of the optical disk 15.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

【特許請求の範囲】

【請求項1】 着脱可能な記録媒体に情報を記録または再生する情報処理装置において、前記記録媒体のIDを読み出す第1の読出手段と、所定の時変情報を発生する発生手段と、前記第1の読出手段により読み出された前記記録媒体のID、および、前記発生手段が発生した前記時変情報を、互いに対応させて第1のテーブルに記憶させる記憶手段と、前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生手段が発生した前記時変情報を、互いに対応させて、前記記録媒体の第2のテーブルに記録させる記録手段と、前記記録媒体の第2のテーブルを読み出す第2の読出手段と、前記第1のテーブルの内容と、第2の読出手段が読み出した前記第2のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御手段とを備えることを特徴とする情報処理装置。

【請求項2】 着脱可能な記録媒体に情報を記録または再生する情報処理方法において、前記記録媒体のIDを読み出す第1の読出ステップと、所定の時変情報を発生する発生ステップと、前記第1の読出ステップで読み出された前記記録媒体のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて第1のテーブルに記憶させる記憶ステップと、前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて、前記記録媒体の第2のテーブルに記録させる記録ステップと、前記記録媒体の第2のテーブルを読み出す第2の読出ステップと、前記第1のテーブルの内容と、前記第2の読出ステップで読み出した前記第2のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御ステップとを備えることを特徴とする情報処理方法。

【請求項3】 着脱可能な記録媒体に情報を記録または再生する情報処理装置に使用するコンピュータプログラムであって、前記記録媒体のIDを読み出す第1の読出ステップと、所定の時変情報を発生する発生ステップと、前記第1の読出ステップで読み出された前記記録媒体のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて第1のテーブルに記憶させる記憶ステップと、前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて、前記記録媒体

の第2のテーブルに記録させる記録ステップと、前記記録媒体の第2のテーブルを読み出す第2の読出ステップと、前記第1のテーブルの内容と、前記第2の読出ステップで読み出した前記第2のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項4】 情報処理装置に装着され、情報が記録または再生される記録媒体において、前記記録媒体に固有のIDと、装着された前記情報処理装置のIDと、前記情報処理装置が発生した時変情報とが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、提供媒体、および記録媒体に関し、特に、より安全にデータを授受することを可能にする情報処理装置、情報処理方法、提供媒体、および記録媒体に関する。

【0002】

【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまうおそれがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【0003】例えば、ミニディスク（MD）（商標）システムにおいては、SCMS（Serial Copy Management System）と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free, copy once allowed, またはcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコードは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【0004】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【0005】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk (DVD) (商標) システムにおける、コンテンツスランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号を復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【0006】

【発明が解決しようとする課題】しかしながら、上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【0007】また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。なぜなら、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【0008】本発明はこのような状況に鑑みてなされたものであり、記録媒体のIDおよび所定の時変情報を記憶するとともに、記録媒体にアクセスした装置のIDおよび時変情報を記録媒体に記録させ、両者の情報の履歴に基づいてアクセスを制御することで、より安全にデータを授受することを可能にするものである。

【0009】

【課題を解決するための手段】請求項1に記載の情報処理装置は、記録媒体のIDを読み出す第1の読出手段と、所定の時変情報を発生する発生手段と、第1の読出手段により読み出された記録媒体のID、および、発生手段が発生した時変情報を、互いに対応させて第1のテーブルに記憶させる記憶手段と、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生手段が発生した時変情報を、互いに対応させて、記録媒体の第2のテーブルに記録させる記録手段と、記録媒体の第2のテーブルを読み出す第2の読出手段と、第1のテーブルの内容と、第2の読出手段が読み出した第2のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御手段とを備えることを特徴とする。

【0010】請求項2に記載の情報処理方法は、記録媒体のIDを読み出す第1の読出ステップと、所定の時変情報を発生する発生ステップと、第1の読出ステップで読

み出された記録媒体のID、および、発生ステップで発生した時変情報を、互いに対応させて第1のテーブルに記憶させる記憶ステップと、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生ステップで発生した時変情報を、互いに対応させて、記録媒体の第2のテーブルに記録させる記録ステップと、記録媒体の第2のテーブルを読み出す第2の読出ステップと、第1のテーブルの内容と、第2の読出ステップで読み出した第2のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御ステップとを備えることを特徴とする。

【0011】請求項3に記載の提供媒体は、記録媒体のIDを読み出す第1の読出ステップと、所定の時変情報を発生する発生ステップと、第1の読出ステップで読み出された記録媒体のID、および、発生ステップで発生した時変情報を、互いに対応させて第1のテーブルに記憶させる記憶ステップと、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生ステップで発生した時変情報を、互いに対応させて、記録媒体の第2のテーブルに記録させる記録ステップと、記録媒体の第2のテーブルを読み出す第2の読出ステップと、第1のテーブルの内容と、第2の読出ステップで読み出した第2のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【0012】請求項4に記載の記録媒体は、記録媒体に固有のIDと、装着された情報処理装置のIDと、情報処理装置が発生した時変情報とが記録されていることを特徴とする。

【0013】請求項1に記載の情報処理装置、請求項2に記載の情報処理方法、および請求項3に記載の提供媒体においては、記録媒体のIDが読み出され、所定の時変情報が発生され、読み出された記録媒体のID、および、発生された時変情報が、互いに対応して第1のテーブルに記憶される。また、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生した時変情報が、互いに対応して、記録媒体の第2のテーブルに記録され、記録媒体の第2のテーブルが読み出され、第1のテーブルの内容と、読み出された第2のテーブルの内容が比較され、その比較結果に対応して記録媒体に対するアクセスが制御される。

【0014】請求項4に記載の記録媒体においては、記録媒体に固有のID、装着された情報処理装置のID、および情報処理装置が発生した時変情報とが記録される。

【0015】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態(但し一例)を付

加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0016】請求項1に記載の情報処理装置は、記録媒体のIDを読み出す第1の読出手段（例えば、図4のステップS1）と、所定の時変情報を発生する発生手段（例えば、図4のステップS4）と、第1の読出手段により読み出された記録媒体のID、および、発生手段が発生した時変情報を、互いに対応させて第1のテーブルに記憶させる記憶手段（例えば、図4のステップS7、S8）と、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生手段が発生した時変情報を、互いに対応させて、記録媒体の第2のテーブルに記録させる記録手段（例えば、図4のステップS11、S12）と、記録媒体の第2のテーブルを読み出す第2の読出手段（例えば、図4のステップS14）と、第1のテーブルの内容と、第2の読出手段が読み出した第2のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御手段（例えば、図4のステップS13、S18、S19）とを備えることを特徴とする。

【0017】以下、本発明を、光ディスクにデータを記録または再生する光ディスク記録再生装置に適用した第1の実施の形態を、図面を参照しながら説明する。

【0018】図1は、本発明を適用した光ディスク記録再生装置1の構成を示すブロック図である。入力部2は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御回路3は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。EEPROM4は、光ディスク記録再生装置1に固有なID（以下、DeviceIDと称する）、光ディスク記録再生装置1がアクセスした光ディスクの履歴としてのDiscID table、その他、装置の電源オフ後も記憶する必要のある情報を記憶する。

【0019】記録再生回路5は、外部から記録信号の供給を受け取ると、これを変調し、ピックアップ6に供給して、装着された光ディスク15に記録させる。記録再生回路5はまた、ピックアップ6により、光ディスク15から再生されたデータを復調し、外部に再生信号として出力する。ピックアップ6は、レーザビームを光ディスク15に照射することで、データの記録再生を行う。スピンドルモータ8は、サーボ回路7によって制御され、光ディスク15を回転させる。

【0020】サーボ回路7は、スピンドルモータ8を駆動することにより、光ディスク15を所定の速度で（例えば線速度一定で）回転させる。サーボ回路7はまた、ピックアップ6のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路9は、制御回路3の制御により、所定の乱数を発生する。光ディ

スク15は、同図に示すように、通常のコンテンツデータの記録領域であるデータエリア以外に、リードインエリアを有する。リードインエリアには、光ディスクのID（以下、DiscIDと称する）と、光ディスク15に対するアクセス履歴を記憶するDeviceID tableが記録される。

【0021】図2は、DeviceID tableの具体例を示す図である。DeviceID tableは、内部に100個のアドレスを有する。各アドレスには1乃至100の所定のアドレス番号が対応し、1から100まで昇順で、光ディスク15にアクセスした装置のDeviceID、アクセス毎に発生された乱数（詳細は後述する）、および、（最終書き込みアドレスを示す）最終書き込みフラグが、アクセス毎に書き込まれる。なお、アドレス番号が100に達したら、次は再び1に戻り、対応するデータも更新される。

【0022】図3は、DiscID tableの具体例を示す図である。DiscID tableは、内部に100個のアドレスを有する。各アドレスには1乃至100の所定のアドレス番号が対応し、1から100まで昇順で、光ディスク記録再生装置1がアクセスした光ディスクのDiscID、アクセス毎に発生した乱数、および、最終書き込みフラグが、アクセス毎に書き込まれる。なお、アドレス番号が100に達したら、次は再び1に戻り、対応するデータも更新される。

【0023】次に、光ディスク記録再生装置1の光ディスク15に対するアクセスの動作について、図4のフローチャートを参照して説明する。最初にステップS1において、光ディスク記録再生装置1の制御回路3は、ピックアップ6を制御し、光ディスク15のリードインエリアを再生させる。この再生信号は記録再生回路5により復調される。制御回路3はこの復調信号から、光ディスク15のDiscIDとDeviceID tableを読み出し、記憶する。制御回路3は、ステップS2で、EEPROM4のDiscID tableに記憶されたデータを検索する。制御回路3は、ステップS3で、DiscID tableのデータの中に、ステップS1で読み出した光ディスク15のDiscIDと一致するDiscIDがあるか否かを判定する。光ディスク15のDiscIDと一致するDiscIDがないと判定された場合、ステップS4に進み、制御回路3は、乱数発生回路9を制御し、所定の乱数を発生させる。この乱数は、光ディスク記録再生装置1が光ディスク15にアクセスする毎に、個別に発生する時変情報である。この乱数は、制御回路3に供給される。

【0024】制御回路3は、ステップS5で、EEPROM4のDiscID tableを検索し、最終書き込みフラグを検出する。制御回路3は、ステップS6で、最終書き込みフラグが検出されたアドレスよりアドレス番号が1だけインクリメントされたアドレスを、今回のデータ書き込み位置（アドレス）として特定する。但し、アドレス番号は100を超えることはなく、100の次は再び1に戻る。制御回路3は、ステップS7で、ステップS1で読

み取ったDiscIDを、ステップS 6で特定したアドレスに書き込む。さらに制御回路3はステップS 8で、ステップS 4で発生された乱数を、ステップS 6で特定したアドレスに書き込むとともに、最終書き込みフラグを現在のアドレスに書き換える。これにより、DiscIDと乱数が対応して、DiscID tableに書き込まれたことになる。

【0025】制御回路3は、ステップS 9で、光ディスク15のDeviceID table（ステップS 1で読み出している）を検索し、最終書き込みフラグを検出する。制御回路3は、ステップS 10で、最終書き込みフラグが検出されたアドレスより、アドレス番号が1だけインクリメントされたアドレスを、今回のデータ書き込み位置（アドレス）として特定する。制御回路3は、ステップS 11で、EEPROM 4から、光ディスク記録再生装置1のDeviceIDを読み出し、このDeviceIDを、記録再生回路5およびピックアップ6を介して、光ディスク15のDeviceID tableの、ステップS 10で特定したアドレスに書き込ませる。

【0026】制御回路3は、ステップS 4で発生させた乱数を、記録再生回路5およびピックアップ6を介して、光ディスク15のDeviceID tableの、ステップS 10で特定したアドレスに書き込ませるとともに、最終書き込みフラグを現在のアドレスに書き換えさせる。これにより、DeviceIDと乱数が対応してDeviceID tableに書き込まれたことになる。

【0027】次に、ステップS 13に進み、制御回路3は、ピックアップ6を制御して、光ディスク15の入力部2からの指令に対応するユーザデータエリアへアクセスさせ、記録または再生動作を実行させる。すなわち、この場合、制御回路3は、ユーザデータエリアへのアクセス（ユーザデータの記録または再生）を許容する。

【0028】一方、ステップS 3で、光ディスク15から読み取ったDiscIDと同一のDiscIDが、EEPROM 4のDiscID tableに既に記憶されていると判定された場合、ステップS 14に進み、制御回路3は、光ディスク15のDeviceID tableを検索する。制御回路3は、ステップS 15で、光ディスク15のDeviceID tableに、光ディスク記録再生装置1のDeviceIDが記録されているか否かを判定する。光ディスク記録再生装置1のDeviceIDが光ディスク15のDeviceID tableに記録されていると判定された場合、ステップS 16に進み、制御回路3は、光ディスク15のDeviceID tableから、ステップS 15でDeviceIDが検出されたのと同じアドレスにある乱数を読み出す。

【0029】制御回路3は、ステップS 17で、EEPROM 4のDiscID tableから、ステップS 3でDiscIDが検出されたのと同じアドレスにある乱数を読み出す。制御回路3は、ステップS 18で、ステップS 16およびステップS 17で検出された乱数が一致するか否かの判定を行う。両者の乱数が一致しないと判定された場合、また

は、ステップS 15で、光ディスク記録再生装置1のDeviceIDが光ディスク15のDeviceID tableに記録されていないと判定された場合、ステップS 19に進み、制御回路3は、光ディスク15が不正コピーに係るものであると判断する。制御回路3は、この判断に基づき、記録再生回路5を制御して、ユーザデータ信号の記録または再生を禁止させる。すなわち、この場合、制御回路3は、ユーザデータエリアへのアクセスを拒絶する。

【0030】一方、ステップS 18において、ステップS 16およびステップS 17で読み出された乱数が一致すると判定された場合、図5のステップS 20に進み、制御回路3は、以降ステップS 28に至るまでの処理を実行するよう各回路を制御する。なお、図5のステップS 20乃至S 28の処理は、図4のステップS 4乃至S 12の処理と同様の処理である。この場合、ステップS 23およびS 27において、DiscIDおよびDeviceIDは、図4のステップS 3およびS 15で読み出されたものと同一のものが書き込まれる。これに対し、ステップS 20において、乱数は、図4のステップS 17およびS 18で読み出されたものとは異なるものが発生され、ステップS 24およびS 28において書き換えられる。ステップS 28の処理の終了後は、図4のステップS 13に戻り、制御回路3は、以下同様の処理を実行する。

【0031】例えば、ステップS 8で乱数が書き込まれた後、再び、光ディスク記録再生装置1が光ディスク15にアクセスした場合には、ステップS 3、およびステップS 15でYESと判定されて、ステップS 16、S 17に進み、制御回路3により、乱数が読み出され、ステップS 18で、アクセスが許容されることになる。しかしながら、光ディスク15のIDを不正にコピーした光ディスクが、光記録再生装置1に装着された場合には、仮に、光ディスク記録再生装置のDeviceIDが不正にコピーされていたとしても、ステップS 15は（そこでYESと判定されて）通過できるが、ステップS 18で、時変情報である乱数が一致しないと判定されてしまうので、ユーザデータへのアクセスが拒絶されることになる。

【0032】以上のようにして、DiscID tableのDiscIDおよび乱数と、DeviceID tableのDeviceIDおよび乱数を比較し、その一致を検査するようにしたので、ユーザデータエリアへの不正なアクセスに対する防止機能を高めることができる。

【0033】ところで、コンテンツデータを図6に示すように暗号化することで、不正コピーに対する防御効果をより一層高めることが可能である。

【0034】すなわち、図6の例では、光ディスク15のリードインエリアには、DiscIDとDeviceID tableの他、ディスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが格納されている。

【0035】なお、イフェクティブマスタキーKemは、式（1）に従い、マスタキーKmとDiscIDの結合にhash関

数を適用して計算される。ここで、AとBの結合とは、例えば、Aが32ビットで構成され、Bも32ビットで

$$\text{イフェクティブマスタキー}K_{em} = \text{hash}(\text{マスタキー}K_m + \text{DiscID}) \quad (1)$$

ここでマスタキー K_m は、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。データエリアの各セクタ S_i は、ヘッダおよびメインデータ部で構成され、ヘッダには、（セクタ毎に異なる）セクタキー K_{si} をディスクキー K_d で暗号化した暗号化セクタキー EK_{si} ($i=1, 2, \dots$) が格納されている（ここで K_{si} の i は、セクタの番号を示し、セクタキーはセクタ毎に異なるので K_{si} と記述するが、特に区別する必要がない場合は、 K_s とも記述する）。メインデータ部には、コンテンツデータをセクタキー K_{si} で暗号化した暗号化コンテンツデータが格納されている。

【0036】次に、図6のようにしてデータが記録されている光ディスク15を、記録再生する光ディスク記録再生装置1の構成例を、図7に示す。この例では、記録再生回路5が復号部60と暗号化部61を有している。その他の構成は図1における場合と同様である。

【0037】図8は、復号部60の内部の構成を示す図である。Kem発生モジュール81のKmメモリ85は、マスタキー K_m を記憶する。Kem発生モジュール81のhash関数回路86は、マスタキー K_m とDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキー K_{em} を計算する。EKd復号回路82は、光ディスク15から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキー K_{em} で復号して、ディスクキー K_d を計算する。EKs復号回路83は、光ディスク15から各セクタ S_i のヘッダの暗号化セクタキーEK $_{si}$ を読み出し、ディスクキー K_d で復号して、セクタキー K_{si} を計算する。コンテンツデータ復号回路84は、光ディスク15から読み出された暗号化されたコンテンツデータを、セクタキー K_{si} で復号する。

【0038】図9は、暗号化部61の内部の構成を示す図である。Kem発生モジュール101のKmメモリ106は、マスタキー K_m を記憶する。Kem発生モジュール101のhash関数回路87は、マスタキー K_m とDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキー K_{em} を計算する。EKd暗号化復号回路102は、光ディスク15から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキー K_{em} で復号して、ディスクキー K_d を得る。乱数発生回路9は、ディスクキー K_d およびセクタキー K_{si} をそれぞれ乱数として発生する。EKd暗号化復号回路102は、ディスクキー K_d を、イフェクティブマスタキー K_{em} で暗号化して、光ディスク15に記録するとともに、光ディスク15から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキー K_{em} で復号する。Ks暗号化回路103は、セクタキー K_{si} をディスクキー K_d で暗号化して暗号化セクタキーEK $_{si}$ を生成し、光ディスク15に記録する。コンテンツデータ暗

構成されるとき、Aの後にBを配置して、64ビットのデータとすることを意味する。

号化回路104は、セクタキー K_{si} で、コンテンツデータを暗号化し、光ディスク15に記録する。

【0039】図7の光ディスク記録再生装置1は、基本的に、図4および図5に示した場合と同様の動作を行うので、その説明は省略する。但し、この光ディスク記録再生装置1は、図4のステップS13でのアクセス動作を、図10または図11のフローチャートに示すように実行する。

【0040】図10は、復号部60により行われる、ユーザデータの再生処理を説明するフローチャートである。最初に、ステップS41において、Kem発生モジュール81のhash関数回路86は、光ディスク15のリードインエリアから読み出されたDiscIDを受け取る。Kem発生モジュール81のhash関数回路86はさらに、ステップS42で、Kmメモリ85からマスタキー K_m を読み出し、上述の式(1)に従い、光ディスク15のDiscID、および、Kmメモリ85から読み出したマスタキー K_m の結合にhash関数を適用してイフェクティブマスタキー K_{em} を計算し、EKd復号回路82に供給する。EKd復号回路82は、ステップS43で、光ディスク15のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路82は、ステップS44で、この読み出された暗号化ディスクキーEKdを、hash関数回路86から受け取ったイフェクティブマスタキー K_{em} で復号して、ディスクキー K_d を計算し、EKs復号回路83に出力する。

【0041】EKs復号回路83は、ステップS45で、光ディスク15のデータエリアから読み出された各セクタの暗号化セクタキーEK $_{si}$ ($i=1, 2, \dots$) を受け取る。EKs復号回路83は、ステップS46で、この読み出された暗号化セクタキーEK $_{si}$ を、EKd復号回路82から受け取ったディスクキー K_d で復号して、セクタキー K_{si} を計算し、コンテンツデータ復号回路84に出力する。コンテンツデータ復号回路84は、ステップS47で、光ディスク15から読み出された暗号化されたコンテンツデータを受け取る。コンテンツデータ復号回路84は、ステップS48で、この読み出されたコンテンツデータを、EKs復号回路83から受け取ったセクタキー K_{si} で復号し、出力する。

【0042】復号部60の各回路は、ステップS49で、光ディスク15のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップS50に進み、復号部60の各回路は、光ディスク15の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS45以降の処理を繰り返す。全てのコンテンツデータが読み出されたら判定

された場合、復号部60の各回路は、全ての処理を終了する。

【0043】図11は、暗号化部61により行われる、ユーザデータの記録処理を説明するフローチャートである。最初に、ステップS71において、Kem発生モジュール101のhash関数回路107は、光ディスク15のリードインエリアから読み出されたDiscIDを受け取る。Kem発生モジュール101のhash関数回路107は、ステップS72で、Kem発生モジュール101のKmメモリ106から、マスタキーKmを読み出す。Kem発生モジュール101のhash関数回路87は、ステップS73で、上述の式(1)に従い、光ディスク15のDiscID、および、Kmメモリ106から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、EKd暗号化復号回路102に供給する。

【0044】EKd暗号化復号回路102は、ステップS74で、光ディスクのリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd暗号化復号回路102は、ステップS75で、光ディスク15のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か(暗号化ディスクキーEKdを受け取ることができたか否か)の判定を行う。暗号化ディスクキーEKdが書き込まれていないと判定された場合、ステップS76に進み、乱数発生回路9は、40ビットの乱数を発生し、ディスクキーKdとして、EKd暗号化復号回路102に出力する。EKd暗号化復号回路102は、ステップS77で、乱数発生回路9から供給されたディスクキーKdを、hash関数回路107から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク15のリードインエリアに記録する。

【0045】ステップS75で、暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップS78に進み、EKd暗号化復号回路102は、この光ディスク15から読み出された暗号化ディスクキーEKdを、hash関数回路107から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。EKd暗号化復号回路102は、ディスクキーKdを、Ks暗号化回路103に出力する。

【0046】ステップS77またはS78の処理の後、乱数発生回路9は、ステップS79で、40ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路103、およびコンテンツデータ暗号化回路104に出力する。Ks暗号化回路103は、ステップS80で、EKd暗号化復号回路102(暗号化ディスクキーEKdが光ディスク15に記録されている場合)、または乱数発生回路9(暗号化ディスクキーEKdが光ディスク15に記録されていない場合)から受け取ったディスクキーKdで、乱数発生回路9から受け取ったセクタキーKsiを暗号化して、暗号化セクタキーEKsiを生成する。Ks暗号化回路1

03は、暗号化セクタキーEKsiを、光ディスク15のデータエリアにあるセクタヘッドに記録する。

【0047】コンテンツデータ暗号化回路104は、ステップS81で、(ステップS79で乱数発生回路9から受け取った)セクタキーKsiにより、コンテンツデータを暗号化し、光ディスク15のデータエリアのメインデータ部に記録する。

【0048】暗号化部61の各回路は、ステップS82で、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータをまだ記録してはいないと判定された場合、ステップS83に進み、暗号化部61の各回路は、光ディスク15の、まだデータを記録していないセクタにアクセスし、ステップS79に戻り、以下同様の処理を繰り返す。ステップS82で、全てのコンテンツデータが記録されたと判定された場合、復号部60の各回路は、全ての処理を終了する。

【0049】以上のようにして、DiscID tableのDiscIDおよび乱数と、DeviceID tableのDeviceIDおよび乱数を比較し、その一致を検査する第1の実施の形態に加えて、第2の実施の形態では、コンテンツデータを暗号化させることでユーザデータエリアへの不正なアクセスをさらに困難にしたので、不正コピーに対する防御効果をさらに高めることができる。

【0050】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【0051】なお、本明細書中において、上記処理を実行するコンピュータプログラムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【0052】

【発明の効果】以上のように、請求項1に記載の情報処理装置、請求項2に記載の情報処理方法、および請求項3に記載の提供媒体によれば、記録媒体に対してアクセスした情報処理装置の第1のテーブルの内容と、記録媒体から読み出された第2のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御するようにしたので、より安全にデータを授受し、著作権者の権利を保護することができる。

【0053】また、請求項4に記載の記録媒体によれば、記録媒体に固有のID、装着された情報処理装置のID、および情報処理装置が発生した時変情報とが記録されるようにしたので、より安全にデータを授受し、著作権者の権利を保護することができる。

【図面の簡単な説明】

【図1】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図2】DeviceID tableの例を示す図である。

【図3】DiscID tableの例を示す図である。

【図4】図1の光ディスク記録再生装置1の動作を説明

するフローチャートである。

【図5】図1の光ディスク記録再生装置1の動作を説明するフローチャートである。

【図6】光ディスクに記録するデータを説明する図である。

【図7】本発明を適用した光ディスク記録再生装置の他の実施の形態の構成を示すブロック図である。

【図8】図7の復号部60の内部の構成を示す図である。

【図9】図7の暗号化部61の内部の構成を示す図である。

【図10】図8の復号部60の動作を説明するフローチャートである。

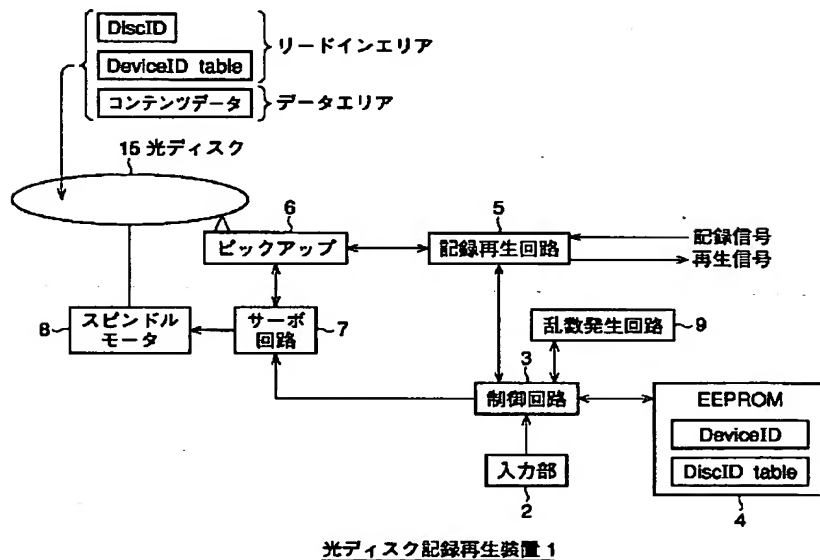
【図11】図9の暗号化部61の動作を説明するフロー

チャートである。

【符号の説明】

1 光ディスク記録再生装置, 2 入力部, 3 制御回路, 4 EEPROM, 5 記録再生回路, 6 ピックアップ, 7 サーボ回路, 8 スピンドルモータ, 9 乱数発生回路, 15 光ディスク, 60 復号部, 61 暗号化部, 81 Kem発生モジュール, 82 EKd復号回路, 83 EKs復号回路, 84 コンテンツデータ復号回路, 85 Kmメモリ, 86 hash関数回路, 101 Kem発生モジュール, 102 EKd暗号化復号回路, 103 Ks暗号化回路, 104 コンテンツデータ暗号化回路, 106 Kmメモリ, 107 hash関数回路

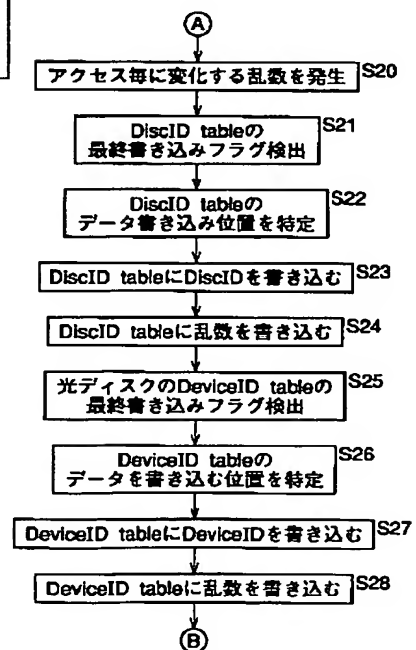
【図1】



【図2】

DeviceID table			
アドレス	DeviceID	乱数	最終書き込み
1			757
2			
...			
100			

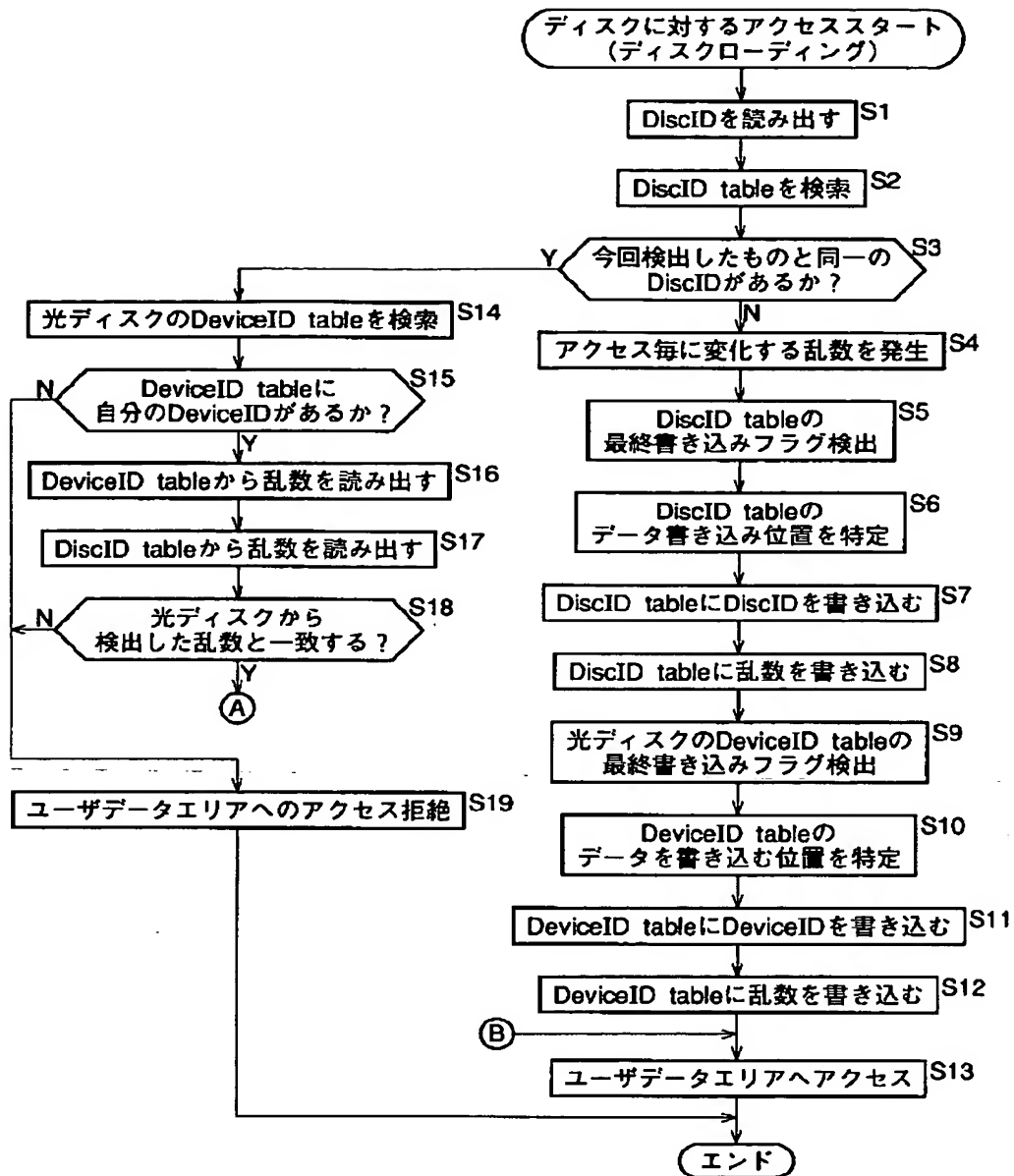
【図5】



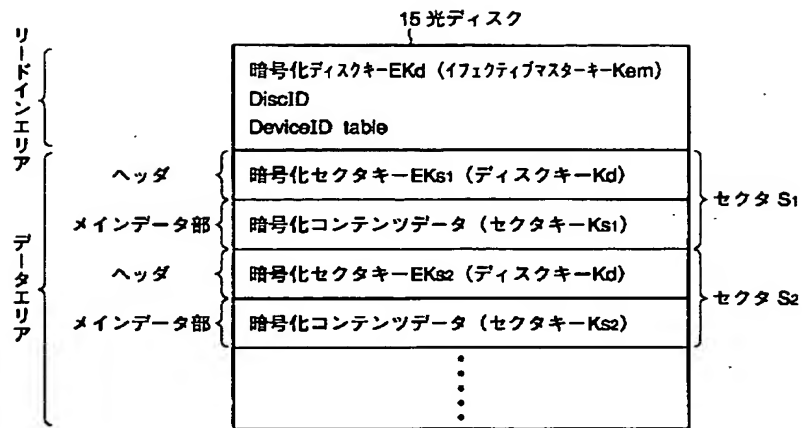
【図3】

DiscID table			
アドレス	DiscID	乱数	最終書き込み フラグ
1			
2			
...			
100			

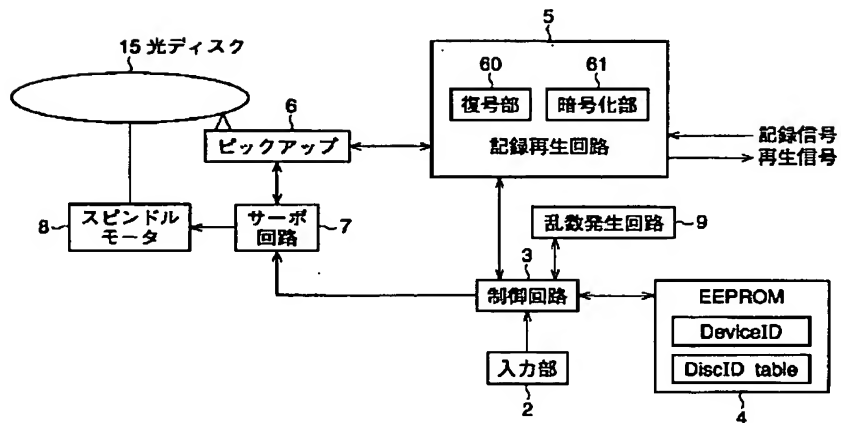
【図4】



【図6】

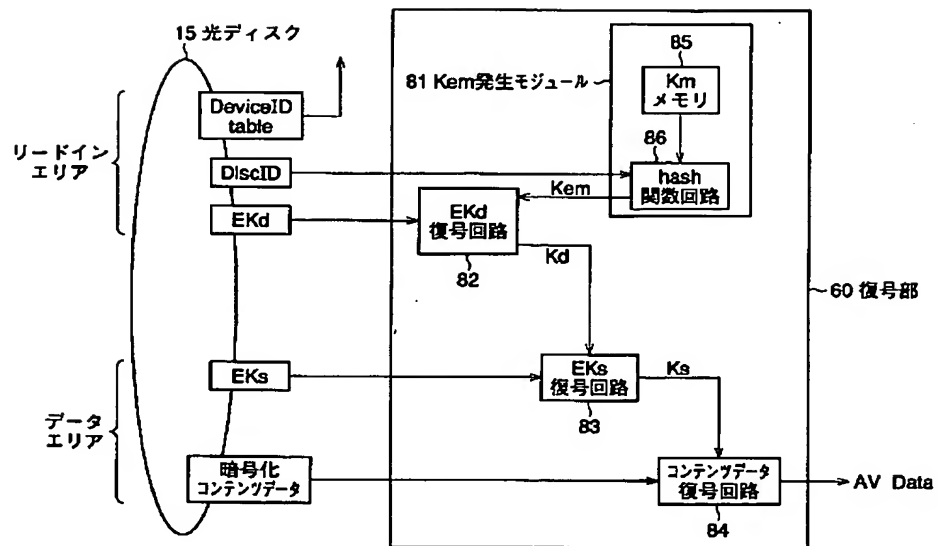


【図7】

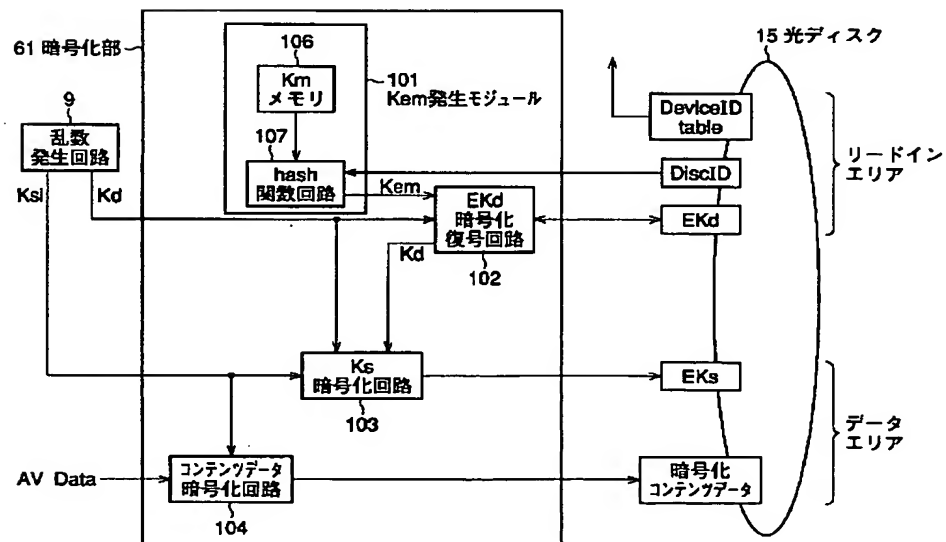


光ディスク記録再生装置 1

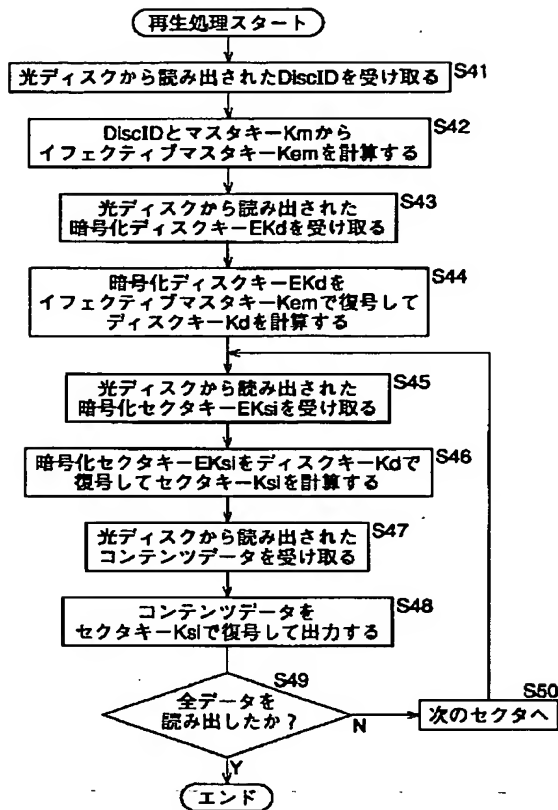
【図8】



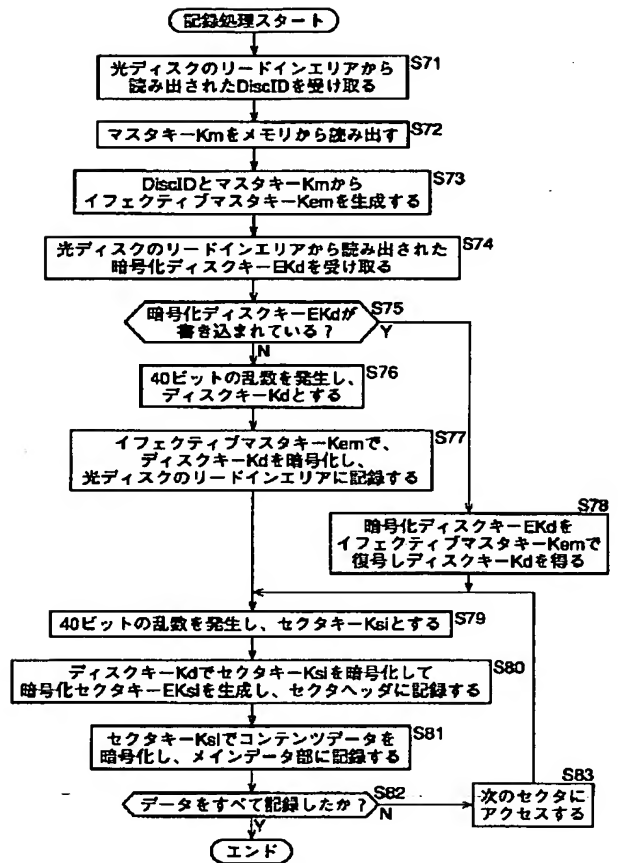
【図9】



【図10】



【図11】



フロントページの続き

(51) Int. Cl.⁶
G 1 1 B 20/12

識別記号

F I
G 1 1 B 20/12